

**UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA**

Stacy Lawton Guin,

Plaintiff,

v.

Brazos Higher Education Service
Corporation, Inc.,

Defendant.

Civ. No. 05-668 (RHK/JSM)

**MEMORANDUM OPINION
AND ORDER**

John H. Goolsby and Thomas J. Lyons Jr., Consumer Justice Center, Little Canada, Minnesota; Thomas J. Lyons, Lyons Law Firm, P.A., Little Canada, Minnesota, for Plaintiff.

Courtney M. Rogers Reid and Matthew E. Johnson, Hallelund Lewis Nilan & Johnson P.A., Minneapolis, Minnesota, for Defendant.

INTRODUCTION

Plaintiff Stacy Guin alleges that Defendant Brazos Higher Education Service Corporation, Inc. (“Brazos”) negligently allowed an employee to keep unencrypted nonpublic customer data on a laptop computer that was stolen from the employee’s home during a burglary on September 24, 2004. This matter comes before the Court on Brazos’s Motion for Summary Judgment pursuant to Federal Rule of Civil Procedure 56. For the reasons set forth below, the Court will grant the Motion.

BACKGROUND

Brazos, a non-profit corporation with headquarters located in Waco, Texas, originates and services student loans. (Villarrial Aff. ¶ 2.) Brazos has approximately 365 employees, including John Wright, who has worked as a financial analyst for the company since November 2003. (Villarrial Aff. ¶ 2; Wright Aff. ¶ 1.) Wright works from an office in his home in Silver Spring, Maryland. (Wright Aff. ¶ 3.) As a financial analyst for Brazos, Wright analyses loan portfolios for a number of transactions, including purchasing portfolios from other lending organizations and selling bonds financed by student loan interest payments. (Wright Aff. ¶ 6.) Prior to performing each new financial analysis, Wright receives an electronic database from Brazos's Finance Department in Texas. (Wright Aff. ¶ 7.) The type of information needed by Wright to perform his analysis depends on the type of transaction anticipated by Brazos. (Wright Aff. ¶¶ 8-11.) When Wright is performing asset-liability management for Brazos, he requires loan-level details, including customer personal information, to complete his work. (Wright Aff. ¶¶ 11.)

On September 24, 2004, Wright's home was burglarized and a number of items were stolen, including the laptop computer issued to Wright by Brazos. (Wright Aff. ¶ 18.) Wright reported the theft to the local police department, but the police were unable to apprehend the burglar or recover the laptop. (Wright Aff. ¶ 19.) After the police concluded their investigation, Brazos hired a private firm, Global Options, Inc., to further investigate the details the burglary. (Villarrial Aff. ¶ 26.) Global Options was unable to regain possession of the computer. (Villarrial Aff. ¶ 26, Ex. 21.)

With the laptop missing, Brazos sought to determine what customer data might have been stored on the hard drive and whether the data was accessible to a third party. Based on internal records, Brazos determined that Wright had received databases containing borrowers' personal information on seven occasions prior to September 24, 2004. (O'Donnell Dep. Tr. at 31-35.) Upon receiving the databases, Wright typically saved the information to his hard drive, depending on the size of the database and the likelihood that he would need to review the information again in the future. (Wright Aff. ¶¶ 14-15.) However, Wright did not keep records of which databases were permanently saved on his hard drive and which databases were eventually deleted, so Brazos was not able to determine with any certainty which individual customers had personal information on Wright's laptop when it was stolen. (Wright Aff. ¶ 16.)

Without the ability to ascertain which specific borrowers might be at risk, Brazos considered whether it should give notice of the theft to all of its customers. In addition to contemplating guidelines recommended by the Federal Trade Commission ("FTC")¹, Brazos learned that it was required by California law to give notice to its customers residing in that State. (Villarrial Aff. ¶¶ 20, 24, Ex. 16.) Brazos ultimately decided to send a notification letter (the "Letter") to all of its approximately 550,000 customers. (Villarrial Aff. Ex. 17.) The Letter advised borrowers that "some personal information

¹ The Federal Trade Commission guidelines recommend that when "deciding if notification [to customers of an identity theft threat] is warranted, [a company should] consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse." (Villarrial Aff. Ex. 16.)

associated with your student loan, including your name, address, social security number and loan balance, may have been inappropriately accessed by the third party.” (Villarrial Aff. Ex. 17.) The Letter also urged borrowers to place “a free 90-day security alert” on their credit bureau files and review consumer assistance materials published by the FTC. (Villarrial Aff. Ex. 17.) In addition, Brazos established a call center to answer further questions from customers and track any reports of identity theft. (Villarrial Aff. ¶ 26.)

Plaintiff Stacy Guin, who acquired a student loan through Brazos in August 2002, received the Letter. (Villarrial Aff. Ex. 2; Guin Dep. Tr. at 9-10.) Shortly thereafter, Guin contacted the Brazos call center to ask followup questions. (Guin. Dep. Tr. 12-15.) Guin also ordered and reviewed copies of his credit reports from the three credit agencies listed in the Letter. (Guin. Dep. Tr. at 24-26.) Guin did not find any indication that a third party had accessed his personal information and, to this date, has not experienced any instance of identity theft or any other type of fraud involving his personal information. (Guin Dep. Tr. at 24-26, 31.) To Brazos’s knowledge, none of its borrowers has experienced any type of fraud as a result of the theft of Wright’s laptop. (Villarrial Aff. ¶ 26.)

On March 2, 2005, Guin commenced this action asserting three claims: (1) breach of contract, (2) breach of fiduciary duty, and (3) negligence. (Compl. ¶¶ 22-33.) On September 12, 2005, Guin voluntarily dismissed his breach of contract and breach of fiduciary duty claims. Guin brings the remaining negligence claim under Fed. R. Civ. P. 23, on behalf of “all other Brazos customers whose confidential information was inappropriately accessed by a third party” (Compl. ¶ 15.)

STANDARD OF REVIEW

Summary judgment is appropriate where there is no genuine issue of material fact, and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c). For purposes of summary judgment, a fact is “material” if its resolution will determine the outcome of the case, and an issue is “genuine” if the evidence is such that a reasonable jury could return a verdict for the non-moving party. See Anderson v. Liberty Lobby Inc., 477 U.S. 242, 248 (1986); Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 586-87 (1986). Upon a motion for summary judgment, the moving party carries the burden of showing there is no genuine issue of material fact, and all evidence and reasonable inferences must be viewed in a light most favorable to the non-moving party. Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986).

ANALYSIS

In his negligence claim, Guin alleges that “[Brazos] owe[d] him a duty to secure [his] private personal information and not put it in peril of loss, theft, or tampering,” and “[Brazos’s] delegation or release of [Guin’s] personal information to others over whom it lacked adequate control, supervision or authority was a result of [Brazos’s] negligence” (Compl. ¶¶ 31-32.) As a result of such conduct, Guin allegedly “suffered out-of-pocket loss, emotional distress, fear and anxiety, consequential and incidental damages.” (Compl. ¶ 33.)

Minnesota courts have defined negligence as the failure to exercise due or reasonable care. Seim v. Garavalia, 306 N.W.2d 806, 810 (Minn. 1981). In order to

prevail on a claim for negligence, a plaintiff must prove four elements: (1) the existence of a duty of care, (2) a breach of that duty, (3) an injury, and (4) the breach of the duty was the proximate cause of the injury. Elder v. Allstate Ins. Co., 341 F. Supp. 2d 1095, 1099 (D. Minn. 2004), citing Lubbers v. Anderson, 539 N.W.2d 398, 401 (Minn. 1995). In support of its instant Motion, Brazos advances three arguments: (1) Brazos did not breach any duty owed to Guin, (2) Guin did not sustain an injury, and (3) Guin cannot establish proximate cause. (Mem. in Supp. at 8-19.) The Court will address each in turn.

1. Breach of Duty

In order to prove a claim for negligence, Guin must show that Brazos breached a legal duty owed to him under the circumstances alleged in this case. A legal duty is defined as an obligation under the law to conform to a particular standard of conduct towards another. See Minneapolis Employees Ret. Fund v. Allison-Williams Co., 519 N.W.2d 176, 182 (Minn. 1994). The standard for ordinary negligence is “the traditional standard of the reasonable man of ordinary prudence.” Seim, 306 N.W.2d at 810. In some negligence cases, however, a duty of care may be established by statute. Anderson v. State, 693 N.W.2d 181, 189-90 (Minn. 2005). In such cases, violation of a statutory-based duty may constitute negligence *per se*. Id. at 190.

Guin argues that the Gramm-Leach-Bliley Act (the “GLB Act”), 15 U.S.C. § 6801, establishes a statutory-based duty for Brazos “to protect the security and confidentiality of customers’ nonpublic personal information.” (Mem. in Opp’n at 8.) For the purposes of this Motion only, Brazos concedes that the GLB Act applies to these circumstances and

establishes a duty of care. (Mem. in Supp. at 15 n.2.) The GLB Act was created “to protect against unauthorized access to or use of such records which could result in substantial harm or inconvenience to any customer [of a financial institution].” 15 U.S.C. § 6801(b)(3).

Under the GLB Act, a financial institution must comply with several objectives, including:

Develop, implement, and maintain a comprehensive written information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue;

Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks; and

Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.

16 C.F.R. § 314.4(a)-(c).

Guin argues that Brazos breached the duty imposed by the GLB Act by (1) “providing Wright with [personal information] that he did not need for the task at hand,” (2) “permitting Wright to continue keeping [personal information] in an unattended, insecure personal residence,” and (3) “allowing Wright to keep [personal information] on his laptop unencrypted.” (Mem. in Opp’n at 10.) Brazos counters that Guin does not have sufficient evidence to prove that it breached a duty by failing to comply with the GLB Act. (Mem. in Supp. at 16.)

The Court concludes that Guin has not presented sufficient evidence from which a fact finder could determine that Brazos failed to comply with the GLB Act. In September 2004, when Wright's home was burglarized and the laptop was stolen, Brazos had written security policies, current risk assessment reports, and proper safeguards for its customers' personal information as required by the GLB Act. (Villarrial Aff. Exs. 1, 3-8, 11, 12.) Brazos authorized Wright to have access to customers' personal information because Wright needed the information to analyze loan portfolios as part of Brazos's asset-liability management function for other lenders. (Wright Aff. ¶¶ 6, 11.) Thus, his access to the personal information was within "the nature and scope of [Brazos's] activities." See 16 C.F.R. § 314.4(a). Furthermore, the GLB Act does not prohibit someone from working with sensitive data on a laptop computer in a home office. Despite Guin's persistent argument that any nonpublic personal information stored on a laptop computer should be encrypted, the GLB Act does not contain any such requirement.² Accordingly, Guin has not presented any evidence showing that Brazos violated the GLB Act requirements.

In addition, Guin argues that Brazos failed to comply with the self-imposed reasonable duty of care listed in Brazos's privacy policy — that Brazos will "restrict access to nonpublic personal information to authorized persons who need to know such

² While it appears that the FTC routinely cautions businesses to "[p]rovide for secure data transmission" when collecting customer information by encrypting such information "in transit," there is nothing in the GLB Act about this standard, and the FTC does not provide regulations regarding whether data should be encrypted when stored on the hard drive of a computer. (Mem. in Supp. at 17-18; Johnson Aff. Ex. 8.)

information.” (Mem. in Opp’n at 11.) Brazos concedes that under this policy, it owed Guin a duty of reasonable care, but argues that it acted with reasonable care in handling Guin’s personal information. (Mem. in Supp. at 14.) The Court agrees. Brazos had policies in place to protect the personal information, trained Wright concerning those policies, and transmitted and used data in accordance with those policies. (Villarrial Aff. Exs. 1, 9-12.) Wright lived in a relatively “safe” neighborhood and took necessary precautions to secure his house from intruders. (Wright Aff. ¶¶ 21-22.) His inability to foresee and deter the specific burglary in September 2004 was not a breach of Brazos’s duty of reasonable care. Because Guin has failed to raise a genuine issue of material fact regarding whether Brazos breached its duty of care, summary judgment is appropriate.

Although Guin’s failure to show that Brazos breached its duty of care provides sufficient grounds for granting Brazos’s Motion for Summary Judgment, the Court will address Brazos’s other two arguments.

2. Injury

In order to prove a claim for negligence, Guin must show that he sustained an injury. See Manion v. Nagin, 394 F.3d 1062, 1067 (8th Cir. 2005) (applying Minnesota law). A plaintiff must suffer some actual loss or damage in order to bring an action for negligence. Carlson v. Rand, 146 N.W.2d 190, 193 (Minn. 1966). “The threat of future harm, not yet realized, will not satisfy the damage requirement.” Reliance Ins. Co. v. Anderson, 322 N.W.2d 604, 607 (Minn. 1982).

Guin argues that he has been injured by identity theft. (Mem. in Opp'n at 13-14.) Under both federal and Minnesota law, identity theft occurs whenever a person "transfers, possesses, or uses" another person's identity "with the intent to commit, aid, or abet any unlawful activity." 18 U.S.C. § 1028(a)(7); Minn. Stat. § 609.527(2). Guin argues that the circumstances of this case fulfill the definition of identity theft because "the burglars [in Wright's home in September 2004] had a criminal intention when they broke in and gained possession of [Guin's] identity information." (Mem. in Opp'n at 14.)

In response, Brazos contends that "any finding that a third party accessed [Guin's] personal information [is] sheer speculation." (Mem. in Supp. at 9.) Brazos points out that the evidentiary record is completely devoid of any disputed facts indicating that Guin's personal information was actually on Wright's laptop at the time it was stolen, or that Guin's personal information is now in the possession of the burglar. (Mem. in Supp. at 8.) Therefore, Brazos argues that Guin cannot show that he has been a victim of identity theft.

The facts of this case are closely analogous to Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005). In Stollenwerk, the defendant's corporate office was burglarized and a number of items stolen, including computer hard drives containing the personal information of defendant's customers. 2005 WL 2465906 at *1. After the burglary, several customers brought suit against the company asserting claims for consumer fraud, invasion of privacy and negligence. Id. at *2. In support of their negligence claim, two plaintiffs relied on the opinion of an expert who described their injury as "an increased risk of experiencing identity fraud for the next seven

years.” Id. at *5 n.2. The district court expressly rejected the expert testimony because “the affidavit of plaintiffs’ expert conclusorily posits that plaintiff’s risk of identity fraud is significantly increased without quantifying the risk.” Stollenwerk, 2005 WL 2465906 at *5. In granting summary judgment for the defendant on the negligence claim, the district court determined that the two plaintiffs had failed to establish an injury for the purpose of proving negligence: “absent evidence that the data was targeted or actually accessed [by the burglars], there is no basis for a reasonable jury to determine that sensitive personal information was significantly exposed.” Id. at *5.

Like Stollenwerk, in this case Guin has failed to present evidence that his personal data was targeted or accessed by the individuals who burglarized Wright’s home in September 2004.³ The record shows that Brazos is uncertain whether Guin’s personal information was even on the hard drive of Wright’s laptop computer at the time it was stolen in September 2004. (Wright Aff. ¶ 16.) To this date, Guin has experienced no instance of identity theft or any other type of fraud involving his personal information. (Guin Dep. Tr. at 24-26, 31.) In fact, to Brazos’s knowledge, none of its borrowers has been the subject of any type of fraud as a result of the theft of Wright’s laptop computer. (Villarrial Aff. ¶ 26.) Furthermore, Guin has provided no evidence that his identity has been “transferred, possessed, or used” by a third party with “with the intent to commit, aid,

³ Also like Stollenwerk, this Court rejects the expert affidavit advanced by Guin to support his negligence claim because the expert’s opinion is conclusory and is based on generalizations that are not supported by the specific facts of this case. (See Hendricks Aff. at 22-26.)

or abet any unlawful activity.” See 18 U.S.C. § 1028(a)(7); Minn. Stat. § 609.527(2). No genuine issue of material fact exists concerning whether Guin has suffered an injury.

Accordingly, he cannot sustain a claim for negligence.

3. Causation

To prevail on his negligence claim, Guin must also show that Brazos’s alleged breach of duty was the proximate cause of his alleged injury. See Lubbers, 539 N.W.2d at 401-02. Proximate cause is defined as “consequences which follow in unbroken sequence, without an intervening efficient cause, from the original negligent act.” Hilligoss v. Cross Cos., 228 N.W.2d 585, 586 (Minn. 1975). As a general rule, the criminal act of a third party is “an intervening efficient cause sufficient to break the chain of causation,” provided that the criminal act was not foreseeable and there was no special relationship between the parties. Funchness v. Cecil Newman Corp., 632 N.W.2d 666, 674 (Minn. 2001). “The question of foreseeability of an intervening act is normally one for the trial court and should be submitted to a jury only where there might be a reasonable difference of opinion.” Hilligoss, 228 N.W.2d at 586.

Guin contends that the September 2004 theft of Brazos’s laptop from Wright’s home was reasonably foreseeable because “allowing confidential information to remain unencrypted on unsecured laptop computers increase[s] the risk of theft.” (Mem. in Opp’n at 24.) Guin argues that “the test of foreseeability is whether the defendant was aware of facts indicating [that] the plaintiff was being exposed to [an] unreasonable risk of harm.” (Mem. in Opp’n at 23.) Guin points to similar laptop thefts in the financial industry and the

increasing problem of widespread identity theft. (Mem. in Opp'n at 24.) Based on this, Guin argues that the theft of Wright's laptop was reasonably foreseeable to Brazos because "a reasonable jury could conclude that the risk of information compromise is common knowledge in the financial industry." (Mem. in Opp'n at 25.)

The Court concludes that the September 2004 theft of Wright's laptop from his home was not reasonably foreseeable to Brazos. In Hilligoss, the Minnesota Supreme Court observed that a high crime rate and the commission of similar crimes in a particular area can establish foreseeability of a subsequent criminal attack. 228 N.W.2d at 548. In this case, however, Wright lived in a relatively "safe" neighborhood and took necessary precautions to secure his house from intruders. (Wright Aff. ¶¶ 21-22.) Wright was unaware of any previous burglaries on his block or in his immediate neighborhood. (Wright Aff. ¶ 22.) There is no indication that Wright or Brazos could have possibly foreseen the burglary which took place on September 24, 2004. A reasonable jury could not infer that the burglary caused Guin any alleged injury; such a conclusion would be the result of speculation and conjecture, not a reasonable inference. See Stollenwerk, 2005 WL 2465906 at *7. Guin cannot establish proximate cause in this case and therefore, his negligence claim fails.

CONCLUSION

Based on the foregoing, and all of the files, records and proceedings herein, it is **ORDERED** that Defendant's Motion for Summary Judgment (Doc. No. 20) is **GRANTED**, and the Complaint (Doc. No. 1) is **DISMISSED WITH PREJUDICE**.

LET JUDGMENT BE ENTERED ACCORDINGLY.

Dated: February 7, 2006

s/Richard H. Kyle
RICHARD H. KYLE
United States District Judge